9th International Command and Control Research and Technology Symposium
Coalition Transformation: An Evolution of People, Processes and Technology to Enhance Interoperability

Agile Coalition Environment (ACE)

Author: Michele McGuire
Space and Naval Warfare Command, Chief Engineer's Office
4301 Pacific Highway
San Diego, California 92110
Phone (858) 537-0192/ Fax (858) 537-0155
michele.mcguire@navy.mil

Co-Author: Dale Daniel
Booz Allen Hamilton
1615 Murray Canyon Road
San Diego, California 92108
Phone (619) 725-6500/ Fax (858) 537-0155
daniel_dale@bah.com

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Agile Coalition Environment (ACE)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Space and Naval Warfare Command,4301 Pacific Highway,San Diego,CA,92110**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**32**	

Abstract. The Agile Coalition Environment (ACE) program consists of a combined synergistic group of emerging network-centric and information assurance (IA) technologies. These combined ACE technologies provide the warfighter with enhanced information sharing, collaborative tools and situational awareness capabilities that are both dynamic and secure. Warfighters have access to all required user applications and multiple security enclaves of information at a single workstation. Interoperability is achieved across all applications, platforms and security domains. ACE is presented as a network capability that can be applied to the Coalition Enterprise Information Exchange System (CENTRIXS) as well as other coalition or Community of Interest (COI) networks that require information sharing across multiple security domains between U.S and coalition forces. ACE technologies have evolved during a four-year spiral development cycle and have targeted warfighters at all levels for improving interoperability and knowledge management for current and future joint and coalition operations. This evolution for developing tomorrows IT capabilities has been based on requirements, technology insertion, operational experimentation and improvements as a result of Joint, Coalition, and Naval Fleet feedback. The United States Pacific Command (USPACOM) is the ACE program's sponsoring organization, and the U.S. Navy Space & Warfare Systems Command (SPAWAR) provides project management and technical support.

Issues. The Agile Coalition Environment (ACE) project is currently focusing on increasing the ability for the warfighter to visualize, share and analyze information quickly, and then make rapid decisions based on that knowledge. Today, access to information and how fast it can be delivered directly equate to combat power and combat effectiveness. Coalition operations require the flexibility to rapidly and securely reconfigure networks and user nodes in near-real time. Stove piped coalition networks are built and torn down on a continuous basis due to changes in the operational and political conditions that affect the force structure. Changing networks takes days or weeks and current operations require a more dynamic approach so that networks can be established or modified in near-real time. U.S. forces and agencies are required to share information between certain coalition partners during some periods and others during other periods. During these operations, there are multiple coalition forces all having separate information sources and databases, command & control (C2) nodes, battlefield sensors, weapon assets and information systems. After-action reports from both Afghanistan and Iraq and other real-world coalition operations continuously highlight the requirement for better interoperability and IT capabilities between coalition forces. Most current command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems are stovepipe systems with parochial interests from various service research & development (R&D) & acquisition organizations. As a result, many current C4ISR systems are redundant and non-interoperable and result in a waste of present and future capital investments in IT systems.[1] ACE is focused on the development of technologies that address these interoperability issues and provide both dynamic and secure network computing capabilities to the joint and coalition warfighter. Today, individual military services and agencies determine their own IT needs. This approach has led to the confusing and complex C4ISR landscape that exists today. ACE has taken an approach for technology innovation that provides interoperability and

[1] Representative Jim Saxton, C4I Interoperability for our Warfighters, 2 January 2004.

integration of current and future IT systems based on Network Centric Warfare (NCW) concepts and Global Information Grid (GIG) standards. Based on these concepts and standards, ACE has developed a strategy for technology development and transition that greatly contributes to the evolution of current IT systems and supports today's NCW environment.

Today's networks do not support the degree of agility, security, and capacity needed to support information assurance and network-centric (NC) operations between U.S. military forces, coalition military forces, and other supporting agencies. Today's network environment consists of multiple independent networks, each supporting a single classification enclave (UNCLAS, SECRET, RELFOR, etc.) or a single communication media (voice, video or data). Also, today's networks are highly segmented and isolated through firewalls that only allow a small number of network connection services to be performed by a large number of users. This highly segmented network topology does not allow usage of advanced distributed computing technologies such as network computing and distributed collaboration. This restrictive environment creates many issues that must be solved. Today's restrictive environment:

- Prevents us from taking advantage of significant advancements in distributed computing and collaboration.
- Prevents us from sharing critical information with our allies, coalition partners and security cooperation members.
- Prevents us from fully sharing information, and collaborating with non-DoD partners such as the Federal Bureau of Investigation, Department of Homeland Security, Department of Intelligence, Federal Emergency Management Agency, and the State Department among many others.
- Drives up cost because we have to create separate networks for each of many security enclaves. Each of these separate networks requires its own suite of clients and servers. Users are forced to move from computer to computer to get their work done. Users are forced to have multiple computers at their workspaces to interface with their network environment.
- Current Type 1 encryption using TACLANES and FASTLANES is very expensive and static since encryption keys cannot be changed dynamically in near-real time.
- For activities outfitted with only one network for coalition operations a shift to use another security enclave requires tedious sanitization and reconfiguration efforts.
- Reduces operational responsiveness because users must move from network to network to share information or manually move the information using cumbersome upload and download processes across enclave boundaries when it can be shared. [2]

ACE has been focused on transforming this restrictive environment into one that provides both flexibility and security and assist in solving the issues listed above. ACE

[2] PACOM CIO Whitepaper, Agile Coalition Environment, 12 November 2004

technologies end goal is to provide a capability that provides the right information to the right person, at the right place and time.

ACE Overview. ACE architecture integrates, federates and secures IT systems of multiple operating systems and security domains and improves information sharing, situational awareness and collaboration between services, coalitions, and other organizations and agencies. ACE combines network-centric server clusters, Ultra Thin Clients (UTCs) (See Figure 1), Diskless Stateless Clients Personal Computers (DSC-PC) and/or traditional PCs, along with a robust security solution consisting of EAL4 certified trusted operating systems and hardware VPNs. The Open-System Architecture (OSA) concept has also been incorporated and enables any operating system and application to be quickly integrated into the ACE architecture allowing for rapid scalability and flexibility. The ACE security solution provides an avant-garde ability to rapidly reconfigure networks of various security domains and communities of interest (COI) globally in near-real time.

Figure 1. Secure Ultra Thin Client

During the first developmental stages of the program, server clusters were developed in a highly available construct and user terminals were designed as thin and stateless (no resident memory). The computing power, data storage, and systems administration were maintained at the backend using distributed server clusters and the user seat was designed with no processor or resident memory. The Secure Ultra Thin Client (SUTC) is the preferred user seat as shown in Figure 1; however, thin clients such as the DSC-PCs or normal PC's can be implemented with the ACE architecture as well depending on the user requirement. The DSC-PC is different than the SUTC because it has an internal processor and some memory for processing very high-speed graphics and real-time applications not suited for the SUTC. The DSC-PC is a thin client that pulls the

operating system and applications across the network so it is still more secure for multi-domain access operations than a traditional PC. Traditional PC's can be implemented on the ACE architecture as well, but whenever security domains are changed, the hardrive must be changed out and the PC must be rebooted to purge any resident memory. This is why the UTC stateless appliances are inherently more secure and easier to maintain than standard PCs since they have no internal computing power or data storage. Like a telephone or appliance, they can be plugged in anywhere on the network and users can access required data based on their user profile stored on a smartcard. The smartcard also provides enhanced mobility so users can transit between user nodes rapidly just by pulling their card and reinserting it into another UTC on the network.

The quality-of-service (QOS) and downtime were also important considerations during the development of initial ACE architectures. Powerful redundant backend session servers and application servers provide the user with equal or better performance than a normal PC as documented during numerous experimentation and demonstration venues. All the user visualizes on their screen is a redirected display from respective application servers (e.g. MS Office, GCCS, TBMCS, HPUX, C2PC, etc.). ACE computing has been demonstrated with stateless clients over local area networks (LANs), metropolitan area networks (MANs) and globally over wide area networks (WANs). ACE WAN computing has been accomplished during experimentation and demonstrations. The most recent demonstration venue included Joint Warrior Interoperability Demonstration (JWID) 2003 where the ACE architecture was operated and administered the over a global WAN. Backend servers and security controller devices located at the U.S. Pacific Command in Hawaii provided applications to warfighters on stateless clients at sites including Australia, New Zealand, Canada, Continental United States (California & Virginia) and the United Kingdom. The ACE JWID system performed well for a 30-day period and received positive feedback from the joint, allied, and government agency organizations. The JWID Joint Staff representatives recommended in the JWID 2003 Final Report that ACE should be fielded to the joint community as soon as possible to assist in solving current DOD IT issues.[3] This report included inputs from the warfighters who used the system during JWID, the National Security Agency (NSA) based on the security aspects, the Joint Interoperability Test Command (JITC) on interoperability and the JWID Assessment Working Group.

Dynamic Security Solution (DSS). During the first phases of ACE development, all applications such as MS Office, GCCS, TBMCS, etc. could be accessed from a single display giving the warfighter the ability to access many applications from a single workstation. After combining applications such as UNIX, Windows, etc. to a single display, the next evolutionary step was to combine security levels and communities of interest (COI). Multiple security levels and COIs needed to be accessed simultaneously from a single user stateless workstation.

Another key warfighter requirement in developing the ACE security solution was to provide the capability to rapidly reconfigure the network down to the user level. During high-tempo coalition operations, communities of interest and the coalition force structure

[3] JWID CIT 09.01, JWID 2003 Final Report, JWID Assessment Working Group

changes continuously. Coalition members that are part of today's operations may not be tomorrow. All U.S. Forces may not require a need to know for all U.S. operations. The ACE security solution provides a method to separate data domain networks via encrypted tunnels and provide a method to rapidly establish or exclude certain groups of users within those separate domains as per figure 2. Type 1 encryption is the current method to secure networks. Type 1 hardware includes FASTLANES and TACLANES and whenever a network must be rekeyed because of a compromise or change in coalition force structure, it is currently very difficult to accomplish this rekeying in a timely manner. The ACE architecture includes a Type 2 medium robustness virtual private network (VPN) capability that is dynamic and be changed and rekeyed in near-real time.

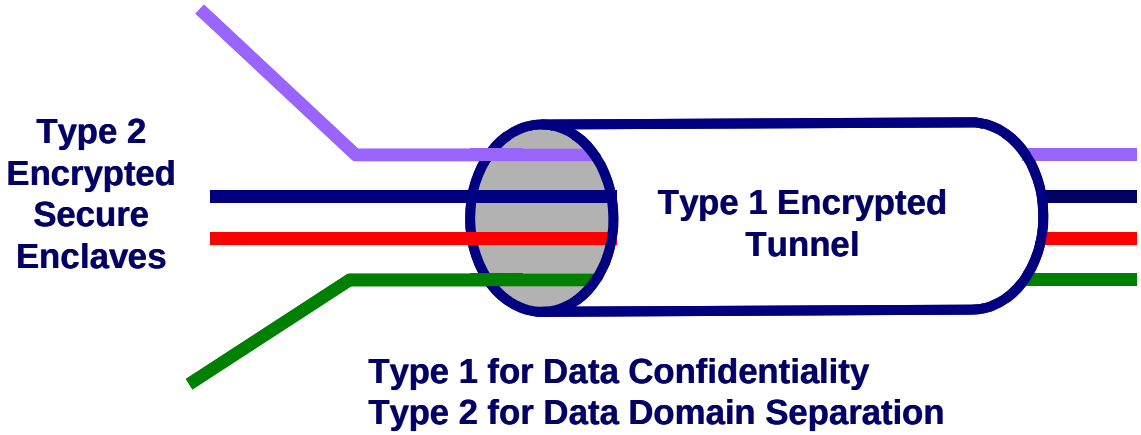


Figure 2. ACE Encryption Method

Trusted operating systems and hardware virtual private network (VPN) devices have been combined to provide data separation within a Type 1 protected environment. These VPN devices allow for dynamic re-keying of the network(s) so that nodes can be added, disabled, or modified in near-real time. The trusted operating system allows for multiple secure domains to be displayed and accessed simultaneously by the user on a single display as shown in Figure 3 below. Strong identification and authentication (I&A) procedures are incorporated via a user smartcard. When a user inserts their smartcard/profile card into the Secure UTC and logs on, they are only allowed access to applications and security domains that they are cleared for. For example a U.S. warfighter may have an access profile that allows access to U.S. Secret and all coalition networks. When the U.S. warfighter inserts their smartcard into the UTC and logs in, they will have access to all networks. When the warfighter is finished with their session, they will logoff and pull their smartcard out of the appliance. Now another warfighter who may only have access to a certain coalition network to the same UTC will insert their smartcard containing their profile and logon and they will only be able to gain access to their particular network domain and data and no other.

Figure 3. Multi Security Domain User Display

.

ACE Capabilities. ACE provides the warfighter with new transformational capabilities that are currently not available with current C4ISR systems. These enhanced capabilities include the following:

a. Enhances interoperability between Joint, Coalition and other agencies by providing a means to share data, provide situational awareness and collaboration simultaneously.

b. Provides a single seat solution for multiple security domains & COI providing broad or restricted access based on user profile.

c. Provides global network operation and global security management.

d. Provides highly available redundant architecture at all levels to ensure continuous access to required data.

e. Provides dynamically reconfigurable network domains by adding/deleting/disabling/ modifying user node profiles globally and in near-real time.

f. Provides interoperability across domains, applications, and platforms.

g. Provides strong integrated identification and authentication (I&A) via trusted operating systems and EAL4 rated VPN devices for data separation.

h. Reduces total ownership costs (TOC) to include reducing space, weight, costs, heat, power and systems administration requirements.

i. Provides easy scalability to meet operational requirements and global force structure.

j. Provides the warfighter with a wide range of value added capabilities via an effective technology transition program.

k. Provides the right information to the right person at the right place at the right time in order to make the right decision and ultimately increase speed of command and control and enhance operational effectiveness

Planned Implementations. Currently, USPACOM and SPAWAR team are implementing an ACE system in PACOM's Standing Joint Forces Headquarters (SJFHQ) on Ford Island, Hawaii. The SJFHQ was designed to maintain an initial Joint Task Force staff that will monitor the PACOM Theater and remain ready to deploy to contingency locations as an initial JTF enabler. The SJFHQ building has limited space and various members of the staff are required to monitor several networks to retain situational awareness and share information and collaborate with allied coalition forces. Once the ACE architecture has been installed and accredited, the SJFHQ staff will have simultaneous access to the following networks at a single UTC display:

- U.S. Secret
- Coalition Enterprise Information Exchange System (CENTRIXS) Japan
- CENTRIXS Korea
- 4-Eyes (United States, United Kingdom, Canada & Australia)
- Global Counter Terrorism Task Force (GCTF)

The ACE team will conduct operational experimentation with the system and will continue to install other ACE systems in Hawaii. Other planned installations include the PACOM Joint Operations Center (JOC) and the Navy's Fleet Command Center. Additional locations will also be identified and populated with the ACE architecture so that users throughout the Pacific Theater can take advantage of the new capabilities that ACE provides to the warfighter.

Summary. To ensure that ACE develops a system that is not theater dependent and can be implemented globally, ACE will continue to develop architectures based on Network Centric Warfare (NCW) concepts using the Global Information Grid (GIG) standards always keeping the warfighter in mind. An example of how ACE evaluates and implements new technologies originates from inputs such as the one from Major General Keith Stalder, Commanding General of the 1st Marine Expeditionary Force (MEF), who said:

> "C4I is first and foremost about people and enhancing their ability to accomplish the mission in a complex, rapidly changing and dangerous environment"

Besides focusing on just the warfighters in the Pacific Theater, ACE will also continuously provide cross-theater information sharing with other warfighting agencies and support organizations globally seeking feedback and attempting to transform this technology into tomorrows C4ISR standard. It is critical that we as technologists collectively work to eliminate the ad-hoc, patchwork IT environment that exists today by developing systems like ACE. We owe it to our brave men and women in uniform who are on the frontlines and risk their lives to protect America's interests at home and abroad.[4]

[4] Subcommittee hearing, "C4I Interoperability: New Challenges in 21st Century Warfare"

Agile Coalition Environment (ACE)
"Freedom within a Framework"

Michele McGuire
Space & Naval Warfare Systems Command
Office of Chief Engineer (056)

Points of Contact

Sponsor:

U.S. Pacific Command

Mr. Randall Cieslak, CIO

(808) 477-7466

randall.cieslak@pacom.mil

Program Manager:

SPAWAR, Office of Chief Engineer:

Ms. Michele McGuire, O56

(858) 537-0192

michele.mcguire@navy.mil

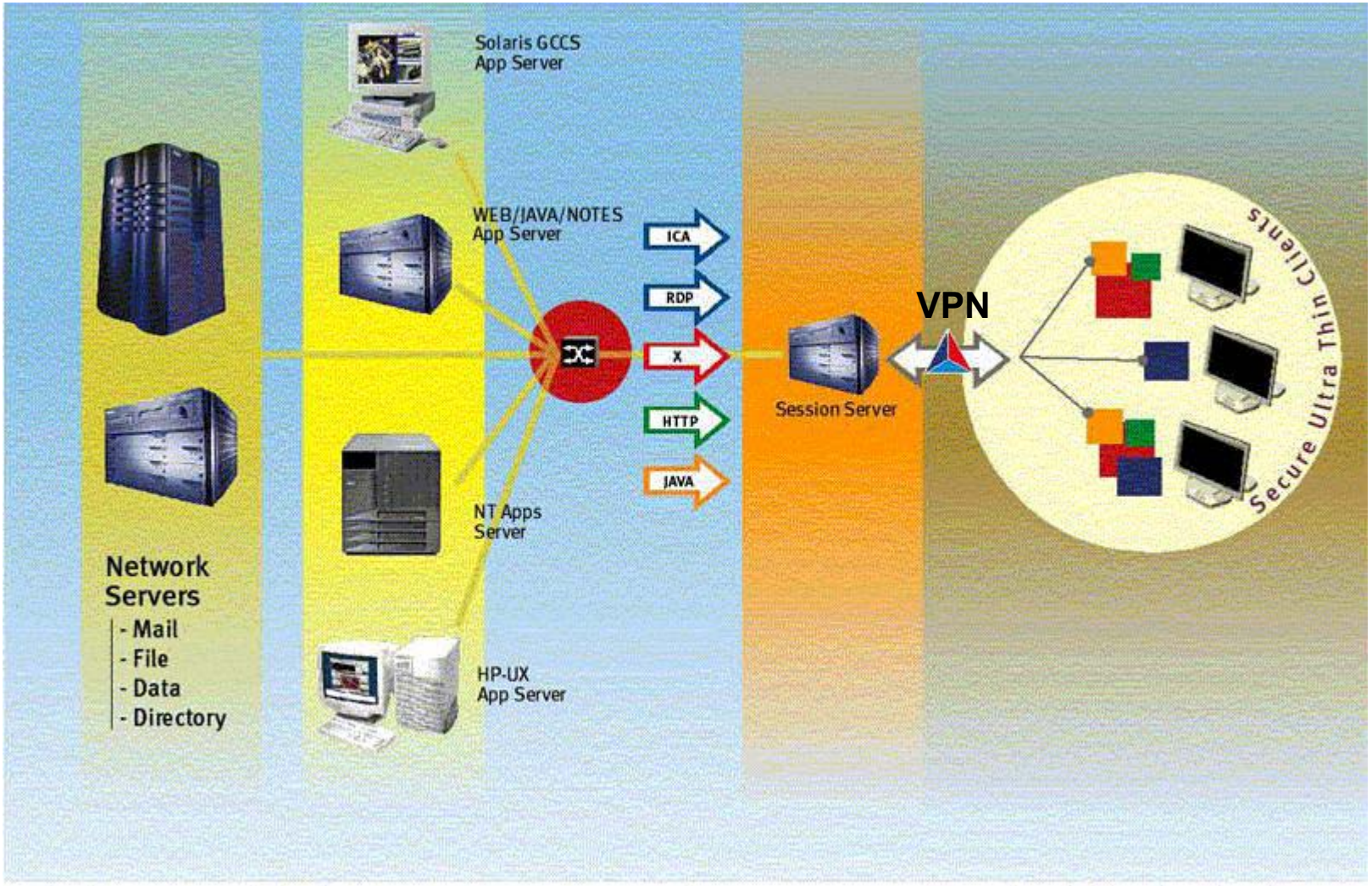
Overview

- Background
- Joint Warrior Interoperability Demonstration (JWID)
- ACE Overview
- ACE Architecture
- ACE Capabilities
- Summary & Questions

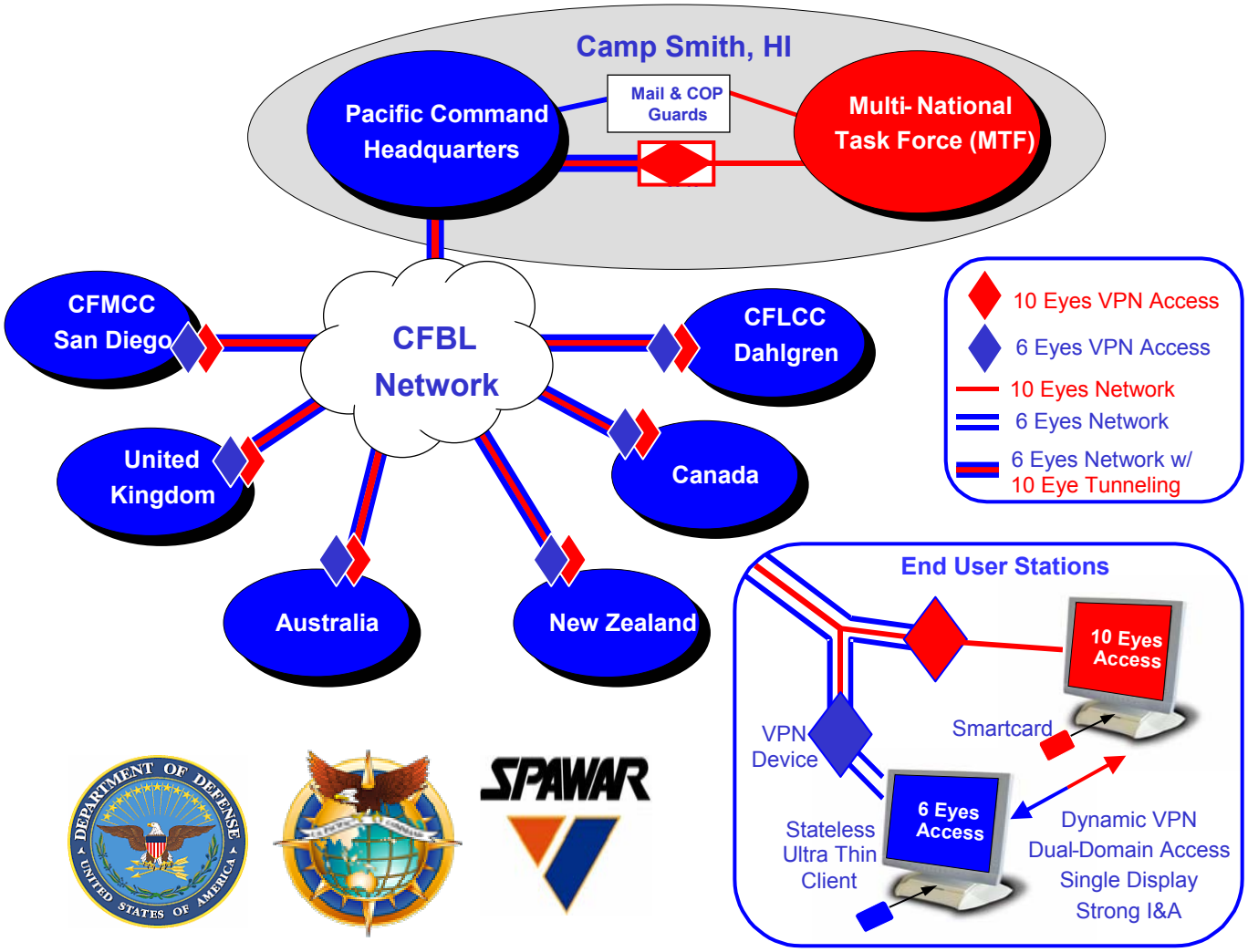
Background

- Technology evolved during 5 years of development & experimentation
  - Network Centric Q-70 Tech Insertion Program w/ Naval Sea Systems Command
  - Space and Naval Warfare (SPAWAR) System Center San Diego Lab
  - USS Coronado Sea Based Battle Lab (SBBL)
  - Fleet Battle Experiment India (FBE I)
  - Joint Warrior Interoperability Demonstrations (JWID) in 2000, 2001, and 2003.
    Pacific Theater Initiative 2002
  - U.S. Pacific Command (PACOM)
    ACE Architecture Development
- Currently in Spiral Development/ Operational Experimentation Phase

Basic Architecture Overview



Experimentation - JWID 03



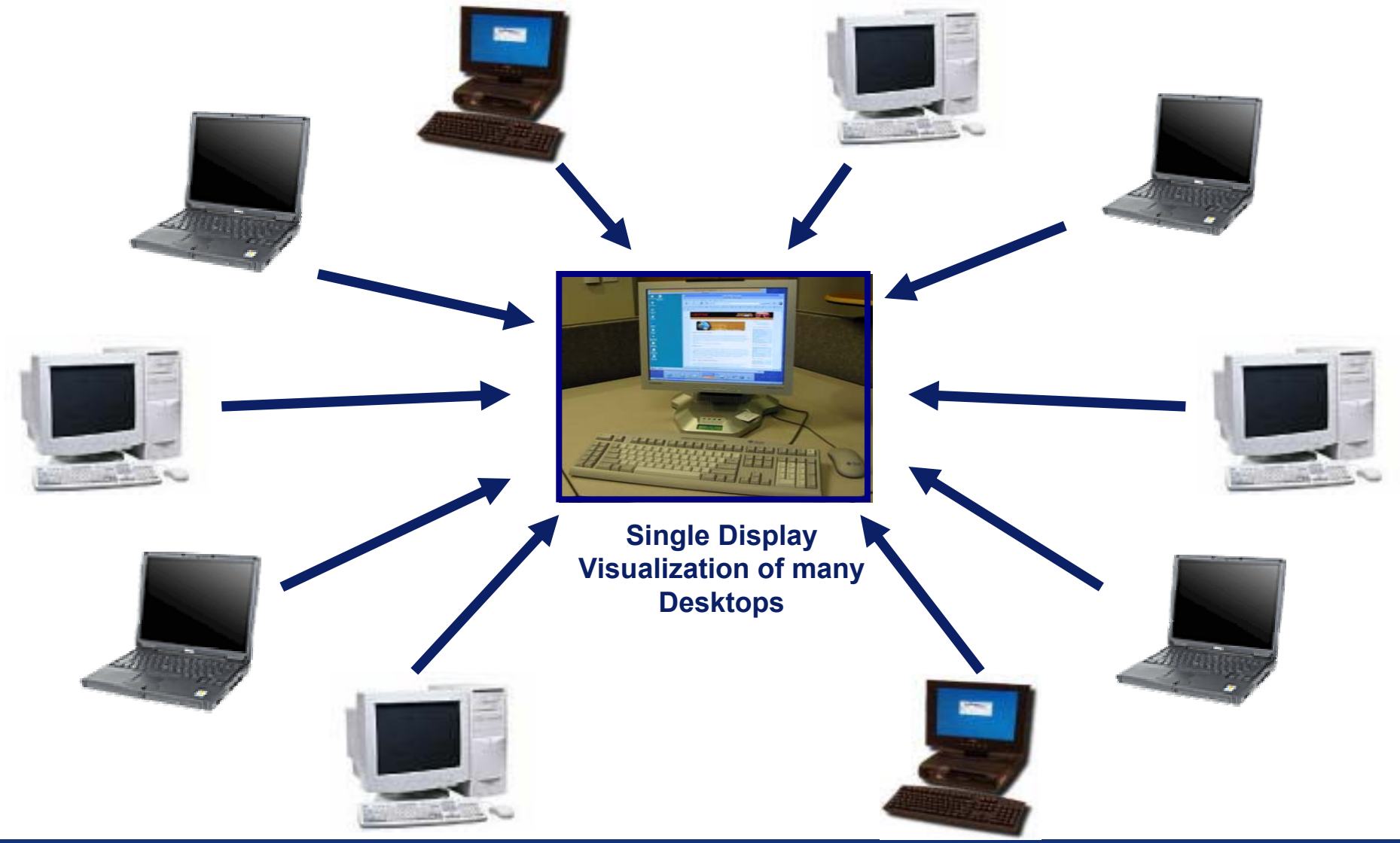
JWID 2003
Benefits & Results

- Benefits:
  - Eliminated need for Type 1 devices for data separation
  - Stateless seats coupled to Enhanced Assurance Level (EAL) 4 certified Virtual Private Network (VPN) devices allow access to multiple domains
  - Server-centric construct used to build centralized and manageable Communities of Interest (COIs)
  - Centralized network management with dynamic re-configuration in near real-time
- Results:
  - Successfully demonstrated data sharing between two domains across 7 sites
  - Successfully provided Coalition Interoperability
  - Successfully provided information sharing between Coalition partners
  - Successfully demonstrated ability to rapidly reconfigure COIs
  - Successfully demonstrated user access control to the network

Agile Coalition Environment

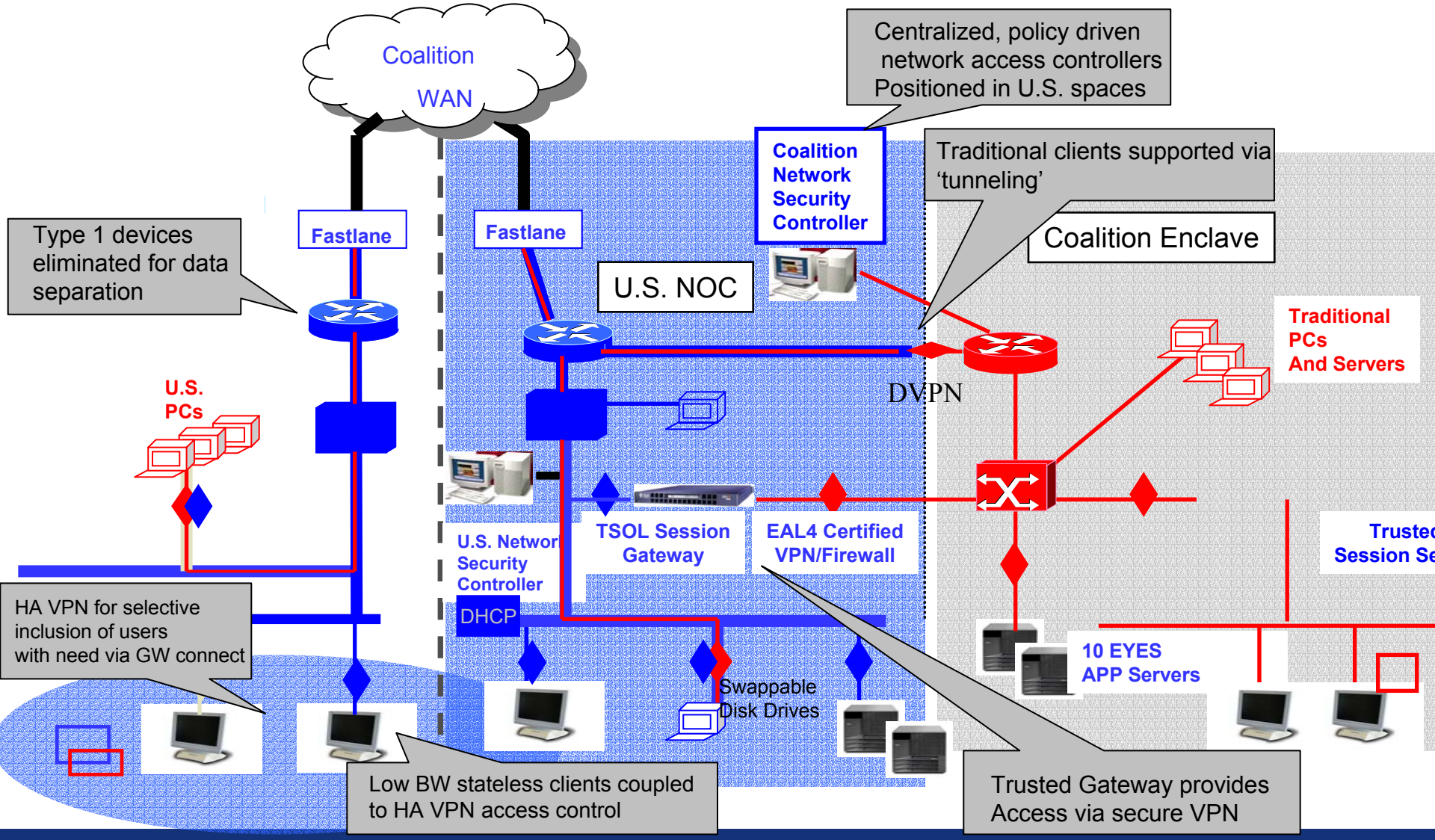
- Technology successfully demonstrated during previous JWIDs
- Network Centric Computing (NCC) plus VPN's & Trusted Solaris (TSol) to consolidate networks & enhance flexibility for rapid reconfiguration
- Integrate High Assurance VPNs onto existing, ubiquitous networks
  - Data domain separation
  - Centralized, policy driven network access control tied to strong 2-factor Identification & Authentication (I&A)
  - Appropriate data encryption for separation vs. confidentiality: Type 2 where appropriate and Type 1 where necessary

Consolidation & Simultaneous Visualization



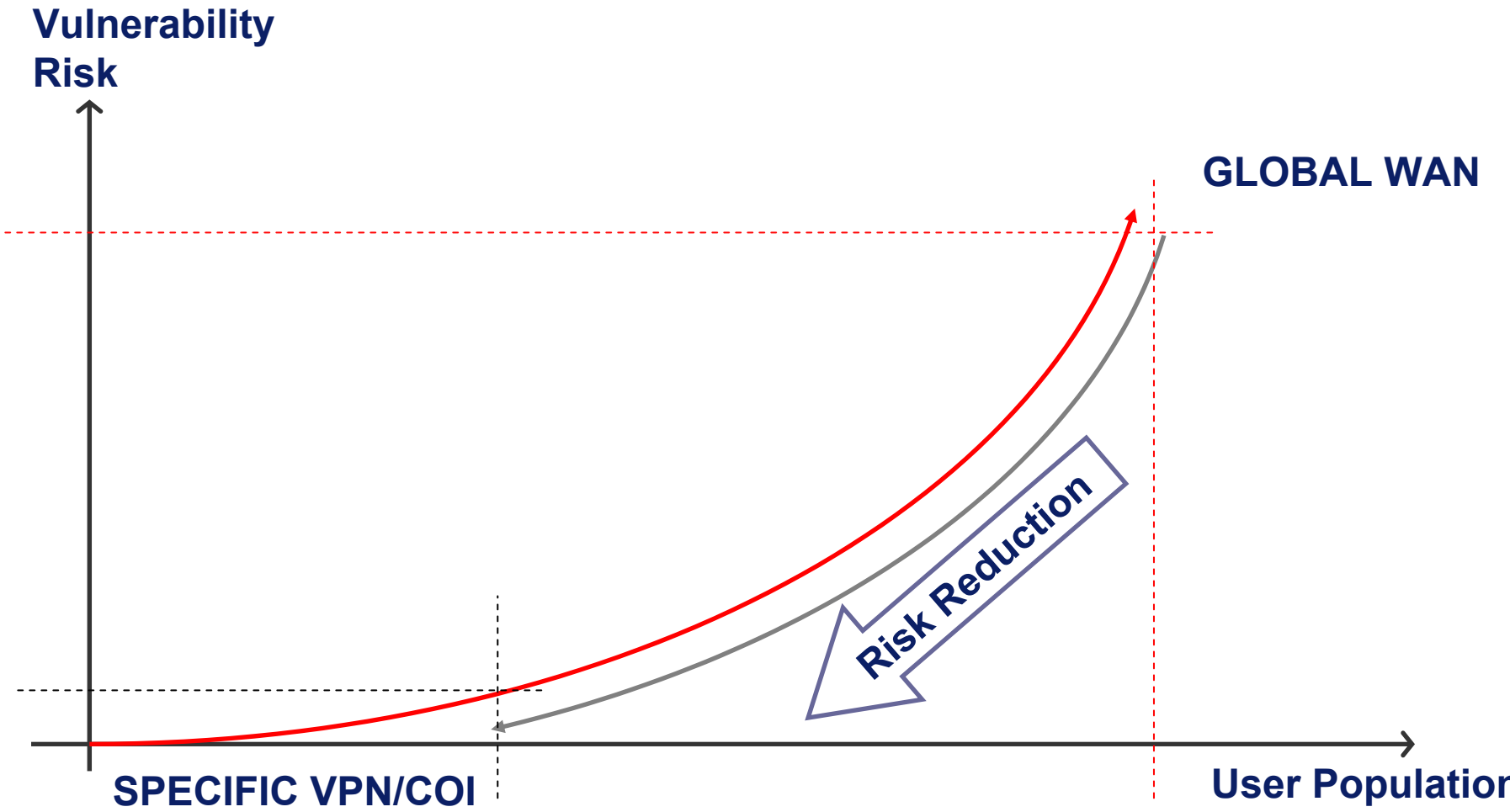
Single Display
Visualization of many
Desktops

ACE Architectural Direction

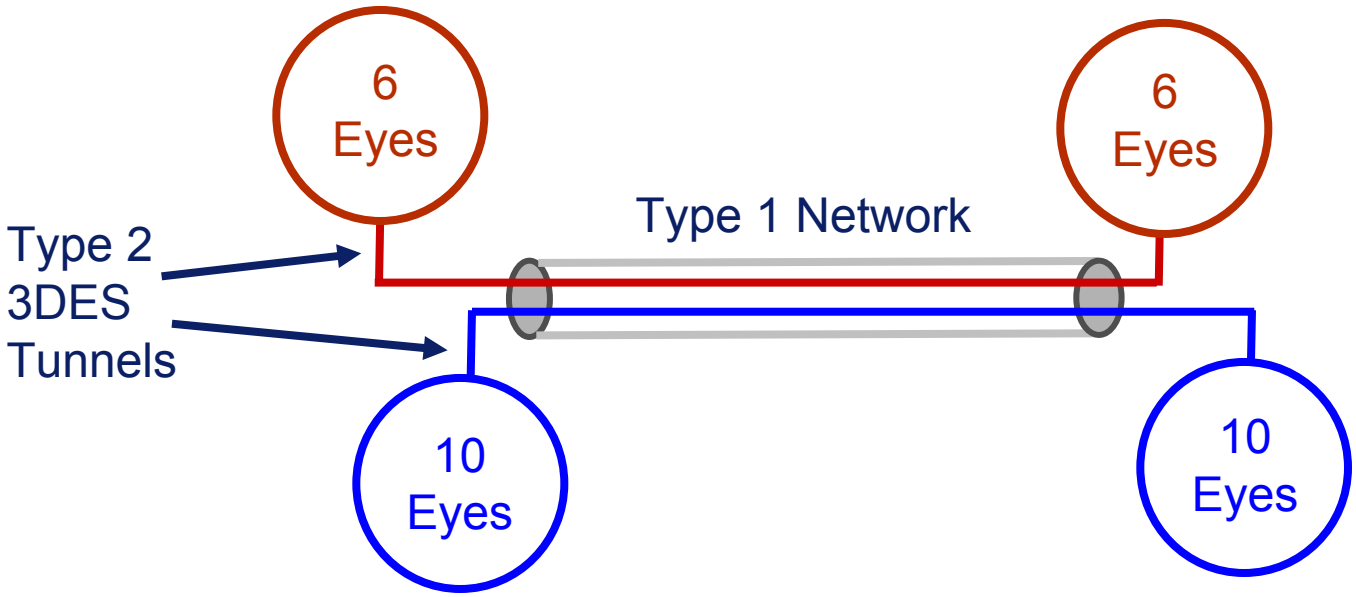


Risk Reduction: Global WAN

STEP 1



Data Separation on Network



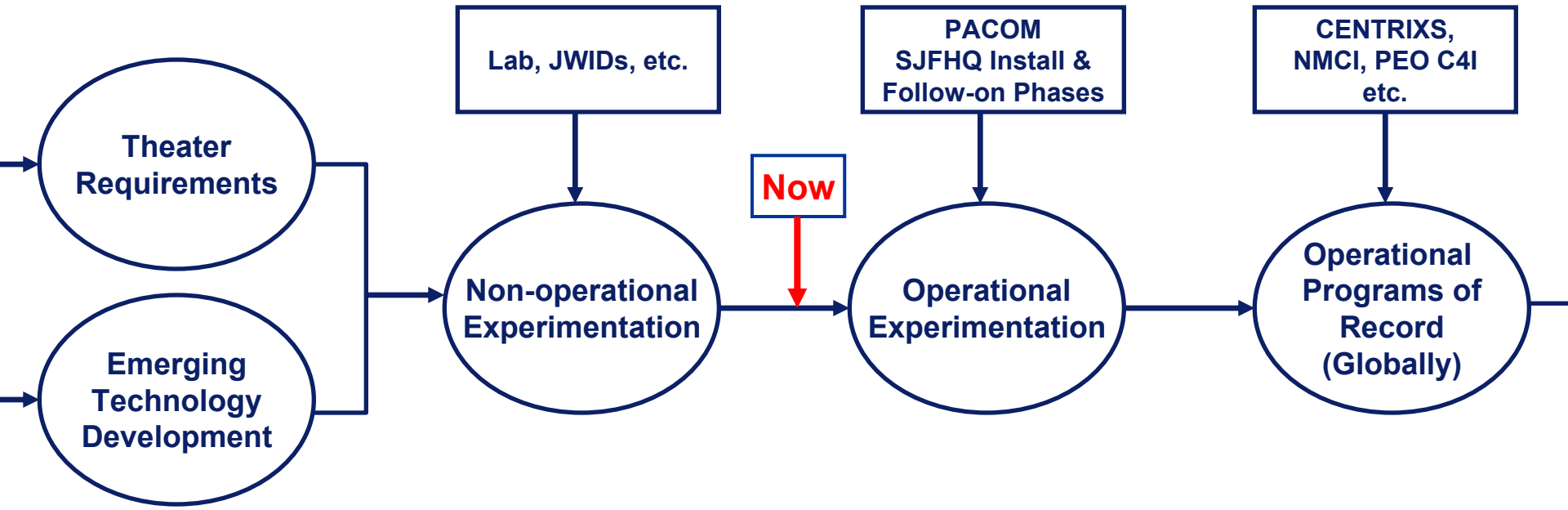
- Concept introduced in Global Information Grid (GIG)
- Tested at Joint Interoperability Test Center & SPAWAR, SSC SD
- Accepted by Coalition Partners
- EAL4 VPN subjected to 6+ months of internal NSA testing and evaluation – NSA approved for JWID Proof-of-Concept

High Assurance VPN Objectives & Benefits

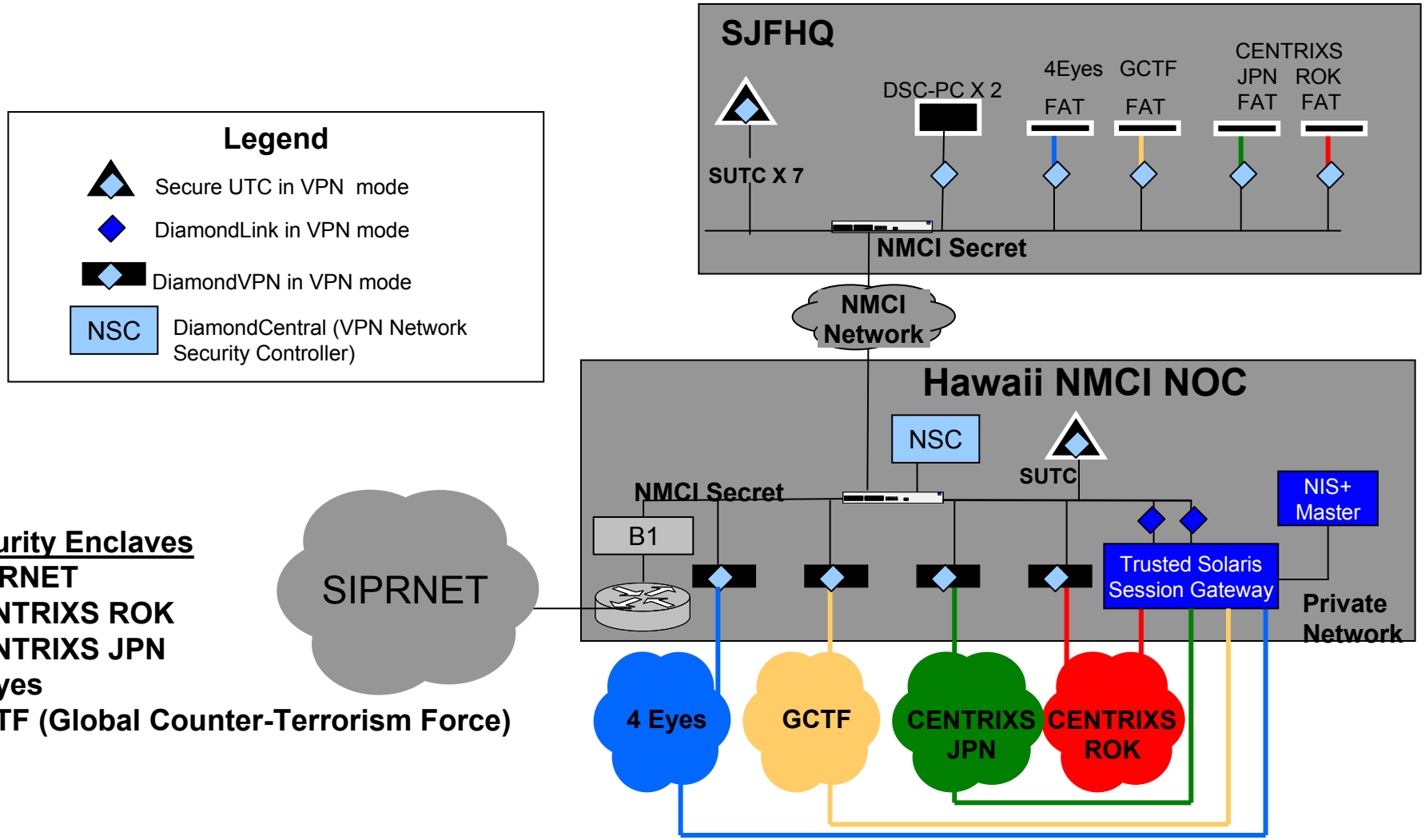
- Objectives:
  - Integrate High Assurance (HA) VPNs onto existing, ubiquitous networks
  - Data domain separation
  - Centralized, policy driven network access control tied to strong 2-factor Identification & Authentication (I&A)
  - Appropriate data encryption for separation vs. confidentiality
    - **IAW CJCSM 6510.01, DEFENSE-IN-DEPTH: INFORMATION ASSURANCE AND COMPUTER NETWORK DEFENSE**
- Benefits:
  - Secure VPNs provide risk reduction on global WAN
  - Selective inclusion of finite number of nodes
  - Medium robustness encryption for data domain separation within security level
  - Optimizes use of Type 1 encryption for data confidentiality and separation of security levels
  - Very tight network access control
  - Also supports secure access from legacy ‘state’ seats
  - Allows Concept of Operations (CONOPS) to maximize benefit of stateless clients for space, weight, power

Current ACE Status

- Warfighters, R&D & Acquisition conducting ***coordinated Spiral Development***



ACE Standing Joint Forces HQ (SJFHQ) Architecture

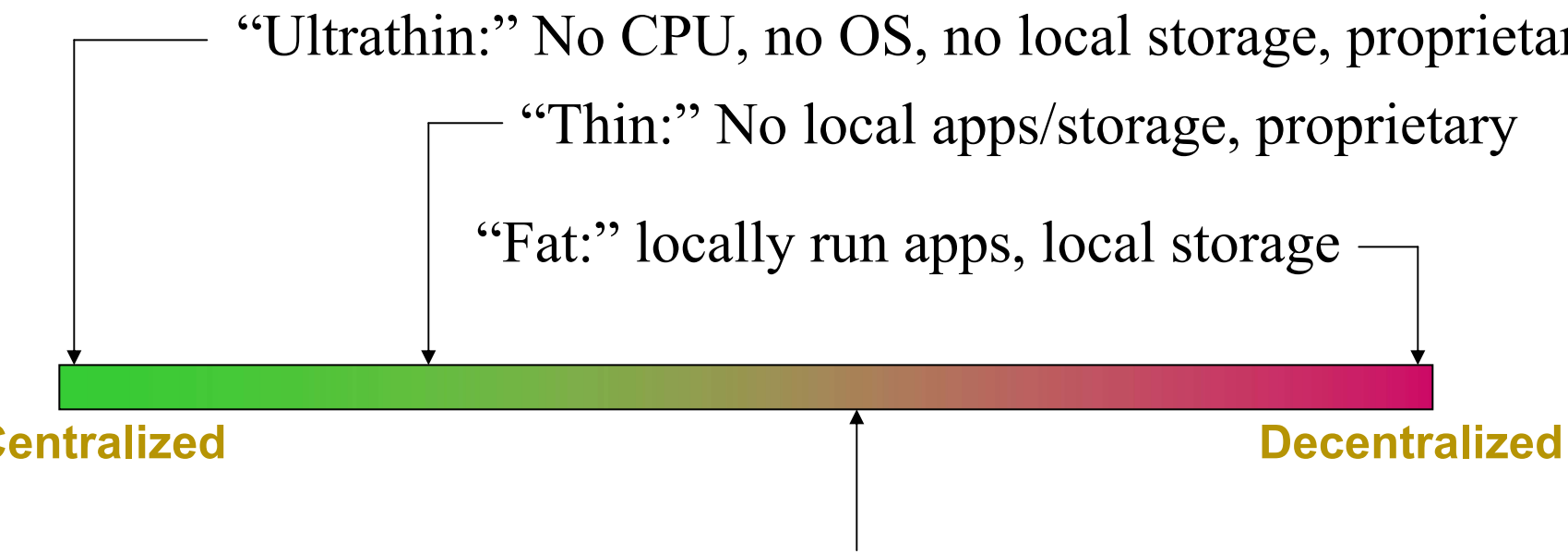


Security Enclaves
- **SIPRNET**
- **CENTRIXS ROK**
- **CENTRIXS JPN**
- **4 Eyes**
- **GCTF (Global Counter-Terrorism Force)**

Secure Ultra Thin Client (SUTC)

- Integration of SunRay and secure VPN technology
- Smartcard maintains user profile for access to network & applications
- Model designed for low-bandwidth ops over WAN
- Lessons learned from JWID 2003 being incorporated
- Inexpensive, multiple purpose and secure seat for global coalition ops
- Simple to manage and operate

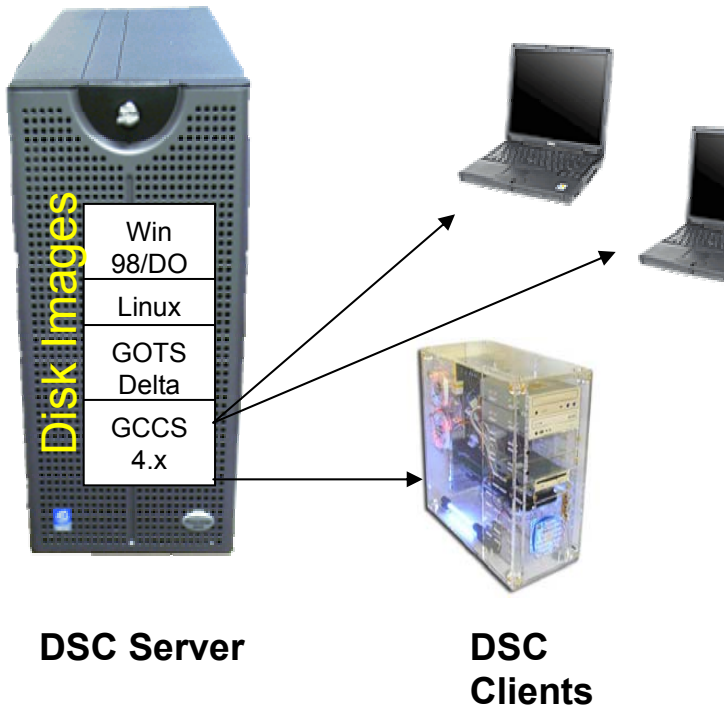
Client Seats



Diskless Stateless Clients (DSC)
Locally run apps, no local storage
Non-proprietary Technology

Diskless Stateless Client (DSC-PC)

- Network load of OS on boot from single VPN domain
- No hard drive locally; uses network-attached storage device at servers
- Local OS for local processing such as audio collaboration
- Use Common Access Card (CAC) card for authentication and for email PKI Certifications
- Provides access to one security enclave at a time
- Allows server-centric management and flexibility to host JAVA based applications such as GCCS-4.x or IWS requiring lots of CPU and memory
- Hardware VPN Provides EAL4/FIPS certified from seat to server gateways



ACE Capabilities Provided to the Warfighter

- Provides improved means to share data, provide situational awareness & collaboration simultaneously
- Provides a single seat solution for
  - Multiple COIs
  - Multiple Operating Systems & Applications
- Provides ability to rapidly reconfigure network globally and in near-real time
  - Dynamic Encryption & Data Labeling
  - Strong I&A
  - Network Centric Computing (NCC) Architecture

ACE Capabilities Provided to the Warfighter

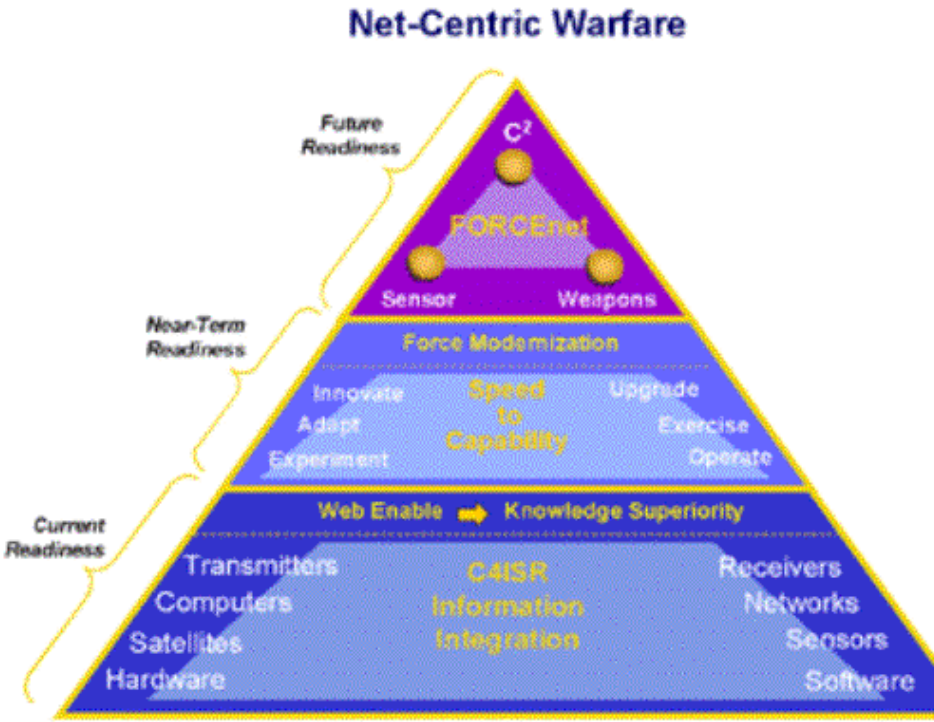
- Reduced Total Ownership Costs (TOC)
- Ease of Scalability to Meet Operational Requirements
- Provides Right Information to the Right Person at the Right Place at the Right Time to Make the Right Decision

Current ACE Status

- Have received Secret and Below Information (SABI) Ticket #
- Cross Domain Appendix (CDA) has been reviewed and approved by NETWARCOM and PACOM
- System Security Authorization Agreement (SSAA) in Draft form
- Have started Pre-CT&E (Certification Test and Evaluation)
- Two groups at NSA have started to review overall architecture and individual component documentation

Summary

- ACE team will continue development & implementations based on:
  - Warfighter Requirements
  - Enhancing Coalition Warfare Capabilities
  - Network Centric Warfare Concepts
  - GIG Standards
- Cross-Theater/Organization/Agency Information Sharing
- Provide the right information, to the right person, at the right place, at the right time to make the right decision



??? Questions ???